UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/759,986	01/16/2004	Erland Wittkotter	W233-US2	8320

7590 07/31/2006

Erland Wittkotter
Apt. 174
25200 Carlos Bee Blvd
Hayward, CA 94542

EXAMINER	
ALMEIDA, DEVIN E	

ART UNIT	PAPER NUMBER
2191	

DATE MAILED: 07/31/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/759,986	WITTKOTTER, ERLAND	
	Examiner	Art Unit	
	Devin Almeida	2191	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 January 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *14 October 2004* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☒ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 20010720
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

This action is in response to the papers filed 1/16/2004. Claims 1-22 were received for consideration. No preliminary amendments for the claims were filed. Currently claims 1-22 are under consideration.

Priority

Acknowledgment is made of applicant's claim for foreign priority under 35 U.S.C. 119(a)-(d). The certified copy has been received.

Information Disclosure Statement

The information disclosure statement (IDS) submitted on 1/14/2004 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Drawings

The drawings are objected to as failing to comply with 37 CFR 1.84(p)(4) because reference character "270" has been used to designate both input unit on page 19 line 16 and timer on page 19 line 23. Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. Each drawing sheet submitted after the filing date of an application must be

labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 1-22 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The claims are generally narrative and indefinite, failing to conform with current U.S. practice. They appear to be a literal translation into English from a foreign document and are replete with grammatical and idiomatic errors.

With respect to claim 1, a device for digital signature of an electronic document by means of a signature creation unit, which is portable and in the form of a card and protected against manipulation. Which is planned for cooperation with a data processing unit for providing the electronic document to be signed and for receiving the digital signature, and which is constructed to deposit the secret, hacker-protected private digital signature encryption, where through a signature processor unit of the signature creation unit, the digital signature can be produced on the basis of a signage string characteristic for the electronic document as well as the private digital signature

encryption. Characterized by, the signature creation unit showing an output unit for giving an output signal for a user of the data processing unit, which cannot be influenced by the data processing unit (examiner construes this to mean that the signature creation unit has an output unit for sending an output signal for the user of the data processing unit). An input unit being associated with the signature creation unit, which can be confirmed by the user (examiner construes this to mean that the input unit is on or connected to the signature creation unit, which the user can input data), and the signature creation unit being formed in such a way, that as a response to the output signal a user input into the input unit is required before the digital signature is created and/or transmitted to the data processing (examiner construes this to mean that the signature creation unit being formed in such a way, that as a response to the output signal a user input into the input unit is required before the digital signature is created or transmitted to the data processing).

With respect to claim 2, characterized by a public digital signature encryption, provided by a certification unit preferably being connected by a data transmission network (examiner construes this to mean that a public digital signature encryption, provided by a certification unit preferably but not having to be connected over a data transmission network), being associated with the private signature encryption, which enables the validation of the private signature encryption by comparison of the characteristic signage string with the digital signature, to which the public digital encryption has been applied.

With respect to claim 3, characterized by an output value, corresponding to the output signal and entered into the input unit by the user (examiner construes this to mean the output unit of the signature creation unit outputs a random number that is displayed and has to be entered into the input unit before the digital signature is created (see page 17 line 22-27 of the specification), being part of the electronic document and being able to be displayed with it after the digital signature was accomplished, or being a part of the output signal of the electronic document, to which the private signature encryption was applied.

With respect to claim 5, characterized by an output value of the output unit as output signal being able to be set or influenced by the input unit (examiner construes this to mean the output unit of the signature creation unit outputs a random number that can be influenced by the input unit) and/or (examiner construes this to be an or) the output unit being connected to the signature creation unit by means of a wireless application, especially over a microwave or light-based connection.

With respect to claim 7, "characterized by the input being physically separate from the signature creation unit." Claim 1 states that "an input unit being associated with the signature creation unit" and claim 7 depends from claim 1. It is unclear how you can be associated with the signature creation unit and also be physically separate from the signature creation unit.

With respect to claim 8, the input unit being connected to the signature creation unit over a wireless application, especially a microwave or light-based connection (examiner construes this to mean input unit is connected to the signature creation unit

over a wireless application that can be but does not have to be a microwave or light-based connection).

This is just some of the examples in the claims that are hard to understand because of the translation. The others claims also have grammatical and idiomatic errors as well and need to be fixed

Regarding claims 2, 11, 13, 15, 16, and 17 the phrase "preferable" renders the claim indefinite because it is unclear whether the limitations following the phrase are part of the claimed invention. See MPEP § 2173.05(d).

Regarding claims 5, 6, and 8 the phrase "especially" renders the claim indefinite because it is unclear whether the limitations following the phrase are part of the claimed invention. See MPEP § 2173.05(d).

Regarding claims 1, 4, and 5 the phrase "and/or" renders the claim indefinite because it is unclear whether the limitations following the phrase are part of the claimed invention. See MPEP § 2173.05(d). For the purpose of applying art and/or will be construed as "or".

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 9 is rejected under 35 U.S.C. 102(b) as being anticipated by Bjerrum (U.S. Patent # 5,311,595). The Bjerrum (U.S. Patent # 5,311,595) reference teaches claim 9, a device for digital signature (column 19 lines 34-45) of an electronic document by means of a signature creation unit, which is portable and in the form of a card (see figure 1 element 124 first electronic card column 11 line 64 – column 12 line 27) and protected against manipulation. Which is planned for cooperation with a data processing unit (see figure 1 element 106 PC column 11 line 64 – column 12 line 27) for providing the electronic document to be signed and for receiving the digital signature (see column 2 lines 35-41 and column 19 line 41-49), and which is constructed to deposit the secret, hacker-protected private digital signature encryption, where through a signature processor unit of the signature creation unit, the digital signature can be produced on the basis of a signage string characteristic for the electronic document as well as the private digital signature encryption (see column 2 lines 57-68). Characterized by, the signature creation unit being formed for storage of a number of private signature encryptions for the same signature process (see column 4 lines 43-49 i.e. encryption key(s) stored in said internal storage of said first electronic card), and the signature creation unit having a selection unit for selection of one of the numbers of private digital encryptions before creating the digital signature, where the selection unit executes the selection as response to one of the digital parameters provided by a parameter storage unit (see column 14 line 63 – column 15 line 11).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1 and 3-6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bjerrum (U.S. Patent # 5,311,595) in view of Caputo et al (U.S. Patent # 5,778,071). The Bjerrum reference teaches claim 1, a device for digital signature (column 19 lines 34-45) of an electronic document by means of a signature creation unit, which is portable and in the form of a card (see figure 1 element 124 first electronic card column 11 line 64 – column 12 line 27) and protected against manipulation. Which is planned for cooperation with a data processing unit (see figure 1 element 106 PC column 11 line 64 – column 12 line 27) for providing the electronic document to be signed and for receiving the digital signature (see column 2 lines 35-41 and column 19 line 41-49), and which is constructed to deposit the secret, hacker-protected private digital signature encryption, where through a signature processor unit of the signature creation unit, the digital signature can be produced on the basis of a signage string characteristic for the electronic document as well as the private digital signature encryption (see column 2 lines 57-68). Characterized by, the signature creation unit (see figure 1 element 124 electronic card) showing an output unit for giving an output signal for a user of the data processing unit, which cannot be influenced by the data processing unit (see column 4 lines 43-56 and column 13 lines 7-33 i.e. processed exclusively by the card). An input unit being associated with the signature creation unit,

which can be confirmed by the user (see figure 1 element 122 station and column 12 lines 22-27, column 13 lines 7-33, and column 21 lines 21-47). The Bjerrum reference does not teach the signature creation unit being formed in such a way, that as a response to the output signal a user input into the input unit is required before the digital signature is created and/or transmitted to the data processing unit. The Caputo reference teaches the signature creation unit being formed in such a way, that as a response to the output signal a user input into the input unit is required before the digital signature is created and/or transmitted to the data processing unit (see column 10 lines 18-50). Therefore it would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to include a PIN or other code to be enter before the transfer is started and include an indication to the user as to whether or not data transferred through device is being encrypted (see column 10 line 32-50). One would be motivated to do this to increase security and make it obvious to the sender that the date is being encrypted.

With respect to claim 3, characterized by an output value, corresponding to the output signal and entered into the input unit by the user, being part of the electronic document and being able to be displayed with it after the digital signature was accomplished, or being a part of the output signal of the electronic document, to which the private signature encryption was applied (see Bjerrum column 3 lines 1-7).

With respect to claim 4, characterized by the input unit being a part of the card and/or module-like signature creation unit or a part of a further data processing unit (see column 13 lines 7-33 i.e. the input/output gate of the electronic card), and not having a

direct physical or logical connection to the data processing unit (see Bjerrum figure 1 element 124 electronic card not have a link with the element 106 PC).

With respect to claim 5, characterized by an output value of the output unit as output signal being able to be set or influenced by the input unit and/or the output unit being connected to the signature creation unit by means of a wireless application, especially over a microwave or light-based connection (see Bjerrum column 21 lines 21-38 and column 22 line 61-67 i.e. the output unit only outputs the digital signature if the correct PIN is entered into the input unit).

With respect to claim 6, the Bjerrum reference does not teach the input unit being constructed for reception of bio identification characteristics, especially for fingerprints, voice or retina of a user. The Caputo reference teaches in addition to a PIN number you can use biological attribute of the user such as a fingerprint (see column 1 line 48-49). There for it would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have conclude that bio identification would make it a lot more secure to users that the person who is sending the digital signature is who they say they are. For the purpose of the way the input unit is being used to gather inputs from the user to make sure that the person using the signature creation unit is the person that the recipient of the digital signature thinks they are. The more tests you make the user of the signature creation take the more likely they are going to be who they say they are. Just making them remember a PIN is easy from anyone watching them input the PIN, remember the PIN and use it

later down the road. With bio identification it is much harder to pretend that you are someone else.

Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over Bjerrum (U.S. Patent # 5,311,595) in view of Caputo et al (U.S. Patent # 5,778,071) and in further view of Sudia (U.S. Patent # 5,659,616). Bjerrum in view of Caputo teaches everything with respect to claim 1 above but with respect to claim 2, it teaches a public digital signature encryption, being associated with the private signature encryption, which enables the validation of the private signature encryption by comparison of the characteristic signage string with the digital signature, to which the public digital encryption has been applied (see Caputo column 3 line 9-27 and column 12 line 23-57). Bjerrum in view of Caputo does not teach that the public digital signature encryption is provided by a certification unit preferably being connected by a data transmission network. Sudia teaches that the public digital signature encryption is provided by a certification unit preferably being connected by a data transmission network (see column 3 line 35-57). There for it would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter to have included a certification unit connected by a data transmission network to ensure that the user is getting the key from a trusted source (see column 3 line 35-47). One would be motivated to use a trusted organization that utilizes digital signature and certificate mechanisms to encode industry-wide security policy and authorization information into the signatures and certificates in order to permit the verifier of the signature to decide

whether to accept the signature or certificates as valid and to reduce the risks associated with digital signature system, particularly with end-user smart cards, by building on this use of public ky certificates and attribute certificates.

Claim 7 and 8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bjerrum (U.S. Patent # 5,311,595) in view of Caputo et al (U.S. Patent # 5,778,071) and in further view of Tolopka (U.S. Patent # 6,044,349). The Bjerrum in view of Caputo reference teaches everything in claim 1 as stated above but with respect to claim 7, does not teach the input unit being physically separate from the signature creation unit and also does not teach with respect to claim 8 the input unit connected to the signature creation unit over a wireless application, especially a microwave or light-based connection. The Tolopka reference teaches the input unit being physically separate from the signature creation unit (see column 8 line 66 – column 9 line 14) and with respect to claim 8 teaches the input unit connected to the signature creation unit over a wireless application, especially a microwave or light-based connection (see column 8 line 66 – column 9 line 14). He also teaches that using wireless card readers make a variety of storage medium configuration possible. There for it would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter to have conclude that the input unit being physically separate from the signature creation unit and the input unit connected to the signature creation unit over a wireless application, especially a microwave or light-based connection, would

have opened up a lot more configurations that can be used such as having smart cards integrated into watches, jewelry and clothing (see column 8 line 66 – column 9 line 14).

Claims 1, 10, 12, 15, 18, 19 and 22 are rejected under 35 U.S.C. 103(a) as being anticipated by Caputo (U.S. Patent # 5,778,071) in view of Di Santo (U.S. Patent # 6,430,691). The Caputo (U.S. Patent # 5,778,071) teaches a device for digital signature (see column 5 lines 18-20) by means of a signature creation unit, which is portable and in the form of a card (see figure 1C element 19 smartcard column 7 lines 1-20) and protected against manipulation. Which is planned for cooperation with a data processing unit for providing the electronic document to be signed and for receiving the digital signature (see column 5 lines 18-27), and which is constructed to deposit the secret, hacker-protected private digital signature encryption, where through a signature processor unit of the signature creation unit, the digital signature can be produced on the basis of a signage string characteristic for the electronic document as well as the private digital signature encryption (see abstract and column 5 lines 7-27). Characterized by, the signature creation unit (see figure 1C element 19 smartcard column 7 lines 1-20) showing an output unit for giving an output signal for a user of the data processing unit, which cannot be influenced by the data processing unit (see column 5 lines 18-27). An input unit being associated with the signature creation unit, which can be confirmed by the user (see column 7 lines 37-61), and the signature creation unit being formed in such a way, that as a response to the output signal a user input into the input unit is required before the digital signature is created and/or

transmitted to the data processing unit (see column 7 line 11-20 i.e. a PIN has to be entered and column 10 line 32 - 50). Caputo does not teach encrypting an electronic document. Di Santo teaches encrypting an electronic document (see column 2 lines 49-56). There for it would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to permit the transfer of at least one computer file between the users, in such case it may again desirable to be able to encrypt the same. Since many users already possess telephones, facsimile machines and computers, it is desirable to provide a security device capable of encrypted and non-encrypted voice, data and facsimile transmission during a single communications session, without requiring a user thereof to commence a separate communications session (see column 1 lines 32-49).

With respect to claim 10, a device for digital signature (see Caputo column 5 lines 18-20) of an electronic document by means of a signature creation unit, which is portable and in the form of a card (see Caputo column 6 lines 43-50) and protected against manipulation. Which is planned for cooperation with a data processing unit for providing the electronic document to be signed and for receiving the digital signature (see column 5 lines 18-27), and which is constructed to deposit the secret, hacker-protected private digital signature encryption, where through a signature processor unit of the signature creation unit, the digital signature can be produced on the basis of a signage string characteristic for the electronic document as well as the private digital signature encryption (see abstract). Characterized by, the signature creation unit being formed for parameter- controlled application of at least one private digital signature

encryption a number of times to the characteristic signage string and/or further signage strings, which are dependent on it or connected to it, where the operating parameters controlling the application provided by an operating parameter storage unit can be generated from data of the electronic document or by a time signal unit or can be input or output externally and a result of the parameter-controlled application can be inserted into a data range of the electronic document before a concluding signing (column 11 lines 56-59).

With respect to claim 12, the digital parameter being selected or determined in a time dependent way and a corresponding time signal being able to be produced either by a time stamp unit of the signature creation unit or by an external timer (see Caputo column 11 lines 56-59).

With respect to claim 15, a device for digital signature (see Caputo column 5 lines 18-20) of an electronic document by means of a signature creation unit, which is portable and in the form of a card (see column 6 lines 43-50) and protected against manipulation. Which is planned for cooperation with a data processing unit for providing the electronic document to be signed and for receiving the digital signature (see column 5 lines 18-27), and which is constructed to deposit the secret, hacker-protected private digital signature encryption, where through a signature processor unit of the signature creation unit, the digital signature can be produced on the basis of a signage string characteristic for the electronic document as well as the private digital signature encryption (see abstract). Characterized by, means being provided for deposit of the digital signature together with an objective time signal and especially with further data in

a signature status server unit preferably connected over an electronic data transmission network, which is protected against manipulation and formed as a storage unit (see column 11 lines 56-59).

With respect to claim 18, a time stamp unit as part of the encryption creation unit, which is provided for producing a digital time signal or for means for receiving a digital time signal and for adding the digital time signal, signed by the digital private encryption, to the electronic document before signing (see column 11 line 56-59).

With respect to claim 19, a text construction unit as part of the encryption creation unit, which is provided for the creation of digital text addition and for adding the means of the digital text addition, signed by means of the digital private encryption, to the electronic document before siring (see column 11 line 60 – column 12 line 13).

With respect to Claim 22, the digital parameters being a calculated document-range specific function, especially applied to segments of an electronic document by an individual signature encryption or a parameter-controlled application of a pre-determined series of signature encryptions, where the document-range specific application is executed by parameter control (see column 11 line 60 – column 12 line 57).

Claim 11, 13, 14, 16 and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Caputo et al (U.S. Patent # 5,778,071) in view of Di Santo (U.S. Patent # 6,430,691) and in further view of Sudia (U.S. Patent # 5,659,616). Caputo in view of Di Santo teaches everything with respect to claim 10 and 15 above but with

respect to claim 11 and 16, it teaches a public digital signature encryption, being associated with the private signature encryption, which enables the validation of the private signature encryption by comparison of the characteristic signage string with the digital signature, to which the public digital encryption has been applied (see column 3 line 9-27 and column 12 line 23-57). Caputo in view of Di Santo does not teach that the public digital signature encryption is provided by a certification unit preferably being connected by a data transmission network. Sudia teaches that the public digital signature encryption is provided by a certification unit preferably being connected by a data transmission network (see column 3 line 35-57). Therefore it would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter to have included a certification unit connected by a data transmission network to ensure that the user is getting the key from a trusted source (see column 3 line 35-47).

With respect to claim 13, Caputo view of Di Santo teaches everything with respect to claim 12 above but with respect to claim 13, it does not teaches the digital parameter and the time signal being deposited and available for validation purposes on an external server unit, preferably connected over a data transmission network, where the server unit reacts as response to a validation inquiry concerning a digital signature with a confirmation signal, without providing the digital parameter to the inquire. The Sudia reference teaches the digital parameter and the time signal being deposited and available for validation purposes on an external server unit, preferably connected over a data transmission network, where the server unit reacts as response to a validation

inquiry concerning a digital signature with a confirmation signal, without providing the digital parameter to the inquire (see column 3 line 35-57 and column 11 line 11 - 67). Therefore it would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter to have validation on an external server unit connected over a transmission network to ensure that the recipient is getting the digital signature from the holder of the private key and not someone else (see column 3 line 11-22).

With respect to claim 14, the Caputo in view of Di Santo reference teaches everything in claim 11, as stated above but with respect to claim 14 does not teach the signature creation unit having means for deleting of such digital parameters, which have a time dependency to the past for the deletion point. Sudia teaches that the age-of-signature attribute restriction, would add more trust to the digital signature since you would be able to set restriction to how long the signature can be valid for different types of transaction (column 4 lines 1-9, column 11 lines 12-41). Therefore it would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter to have conclude that the signature creation unit having means for deleting of such digital parameters, which have a time dependency to the past for the deletion point would add more security and trust to each digital signature. High-value transactions have the age-of-signature attribute period to be quite short, while normal transaction a longer interval. One would be motivated to include this to increase the security for the encryption. If the time set to delete the date is less the time

it would take to break the encryption without the key then security to much stronger then it would be with out an age-of-signature attribute period.

With respect to claim 17, the signature creation unit being formed for additional availability of original data of the electronic document, of compromised or encrypted original data or of structural data associated with the original data, where preferably means for access are provided for this purpose (see Caputo column 14 line 66 – column 15 line 12).

With respect to Claim 20 and 21, the Caputo in view of Di Santo reference teaches everything in claim 15, as stated above but with respect to claim 20 does not teach storing of the digital signature and especially of further data, preferred parameters or time signals being able to be executed on the signature status server unit by the signature creation unit or by the data processing unit, or being executed over structure or metadata within the document as instructions to a document administration unit or with respect to claim 21 the signature status server unit reacting in response to a validation inquiry regarding a digital signature with a confirmation signal, without making the digital parameter stored on the server unit available to the inquirer. Sudia teaches storing of the digital signature and especially of further data, preferred parameters or time signals being able to be executed on the signature status server unit by the signature creation unit or by the data processing unit, or being executed over structure or metadata within the document as instructions to a document administration unit and the signature status server unit reacting in response to a validation inquiry regarding a digital signature with a confirmation signal, without making the digital parameter stored

on the server unit available to the inquirer (see column 11 lines 11-67). There for it would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter to have set up a trusted organization to check the validity of timestamps and digital signatures, and enforce a security policy in order to permit the verifier of a signature to decide whether to accept the signature or certificates as valid (see column 4 line 43-63)

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Devin Almeida whose telephone number is 571-270-1018. The examiner can normally be reached on Monday-Thursday from 7:30 A.M. to 5:00 P.M. The examiner can also be reached on alternate Fridays from 7:30 A.M. to 4:00 P.M.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, David Robertson, can be reached on 571-272-4186. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

DA

Devin Almeida
Patent Examiner
July 19, 2006

DAVID ROBERTSON
SUPERVISORY PATENT EXAMINER